UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/027,714	12/21/2001	David M. Austin	AUZ-002 P	6090

7590 10/04/2005

Wesley L. Austin, Esq.
1987 South Bluebell Drive
Bountiful, UT 84010

EXAMINER	
SZYMANSKI, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/027,714	**Applicant(s)** AUSTIN ET AL.
	Examiner Thomas Szymanski	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) *22-34* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) *22-34* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/21/2001*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

AT

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-21, drawn to a computer program for the detection of an observing program, classified in class 726, subclass 24.

II. Claims 22-29, drawn to Generating system input and then monitoring associated activity for observer programs, classified in class 713, subclass 187.

III. Claims 30-32, drawn to a ciphering program for ciphering the users keystroke input, classified in class 713, subclass 189.

IV. Claims 33-34, drawn to a program for detection of network sniffers, classified in class 713, subclass 153.

The inventions are distinct, each from the other because of the following reasons:

2. Inventions I, II, III and IV are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I has separate utility such as specifically scanning separate portions on the computer system for detection of observer programs, whereas invention II generates false activity and monitors associated responses. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

3. During a telephone conversation with Wesley Austin on 9/19/2005 a provisional election was made without traverse to prosecute the invention of I, claims 1-22. Affirmation of this election must be made by applicant in replying to this Office action. Claims 22-34 withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

4. Claims 1-21 have been examined.

Specification

5. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

6. The applicant is requested to review the specification and update the status of all co-pending applications made mention of, replacing attorney docket numbers with current U.S. application or patent numbers when appropriate. References to U.S. applications or patents should make it clear as to what the number refers (e.g. U.S. Patent No. #), instead of listing only the number.

Drawings

7. Figures 1-2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled

"Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 1-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As stated the subject matter of the above noted claims refers to a computer program that is not stated as being contained within any tangible medium. In order for such subject matter to conform to the statutory basis it must be contained within a computer readable medium or some other form that is tangible.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Togawa U.S. Patent No. 6,240,530, and further in view of Drake U.S. Patent No. 6,006,328.

12. Togawa teaches a system for the detection and removal of computer malware.

13. Togawa fails to teach explicitly searching for observer programs as part of that malware.

14. Drake teaches security methods to protect against attacks on a computer system and its software from such sources as eavesdropping on those computer systems.

15. It is desirable within any computer system to maintain the security and integrity of such a system while preventing damage to the data and components included therein. (Drake Col 3 lines 30-52)

16. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Drake with that of Togawa for the advantages of improved security by adding the features of protection against such malicious activities as eavesdropping to the ability of the scanning system as described by Togawa.

17. Regarding Claims 1 and 21: Observer program data characteristics (Togawa Fig 1.s1, Col 5 lines 10-19 Drake Fig 4,5 Col 3 lines 31-52) As it is understood the detection of a virus and its type as within Togawa requires recognition of characteristics of a virus. Those characteristics residing within the computer systems various components as any particular various infects that system; so then the same is true

within the combined system for the detection of an observer program as defined by Drake.

Obtain memory data of the computer (Togawa Fig 1, Col 8 lines 14-30) As explained above the detection of the malware requires checking the system which is inclusive of the memory data; therefore in order for the functionality to proceed it must in some way obtain such data for scanning.

Comparing memory data with observer program data characteristics for detection of an observer program (Col 8 lines 14-30) As it is known within the art virus scanning is the process of comparing two such sets of data. Further within the combined system the observer program characteristics are included within the set of the compared traits.

Generating a result of whether an observer program is present (Fig 1, Fig 3-4 Col 5 lines 10-38) Detection denotes that a result is generated as to the response of the scanning process.

Presenting results through a GUI (Fig 3-4, Col 5 lines 39-50, Col 13 lines 8-55, Col 14 lines 18-25) As denoted the display performs functions of disseminating operational information which is in a graphical form and presented within an OS that the user is capable of interacting with.

18. Regarding Claims 2 and 3: Memory data includes startup and registry startup commands (Col 8 lines 14-30, Col 13 lines 19-56) As stated the memory contains all necessary information for the processes of the machine; these processes being inclusive of starting up necessary portions for operation thereof; such as the OS which

includes a registry and the virus detection that being its own implementation scans the memory that these commands are located within.

19. Regarding Claims 4 and 5: Observer program characteristics include observer import/export table data for comparison with memory import/export table data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56) As explained above all of the common features of the memory and functionality of the system are scanned via the anti-malware system.

20. Regarding Claim 6: Observer program characteristics include observer resource data for comparison with memory resource data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56)

21. Regarding Claim 7: Observer program characteristics include observer file content data for comparison with memory file content data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56) Additionally, as is shown and well known within the art file content is compared to malware characteristics for detection of such programs located commonly in such a place.

22. Regarding Claim 8: The comparing instruction compare the observer file content data with memory file content data at an offset address (Fig 1, Fig 3-4, Col 5 lines 10-20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore the process must offset the data being scanned by that which has already been.

23. Regarding Claim 9: The comparing instruction compare the observer file content data with a span of the memory file content data identified by an offset address (Fig 1,

Fig 3-4, Col 5 lines 10-20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore that which is scanned is a span of memory that is offset by the amount previously scanned.

24. Regarding Claim 10: Observer program characteristics include observer module loading data for comparison with memory module loading data to determine the presence of an observer program (Col 5 lines 10-20, Col 13 lines 19-56)

25. Regarding Claim 11: Observer program characteristics include OS observing functions for comparison with memory functions from the memory data to determine the presence of an observer program (Col 5 lines 10-20, Col 13 lines 19-56)

26. Regarding Claim 12: Memory data includes explorer extension data (Col 13 lines 19-56)

27. Regarding Claim 13: Memory data includes file use information (Col 13 lines 19-56)

28. Regarding Claim 14: Memory data includes process information (Col 13 lines 19-56)

29. Regarding Claim 15: Memory data includes running process information (Col 13 lines 19-56)

30. Regarding Claim 16: Memory data includes loaded module information (Col 13 lines 19-56)

31. Regarding Claim 17: Memory data includes driver data (Col 13 lines 19-56)

32. Regarding Claim 18: Memory data includes kernel driver data (Col 13 lines 19-56) All of the above stated separate memory data components are included within any

resident memory of a common computer system that a system such as the combination of Togawa and Drake would be implemented upon.

33. Regarding Claims 19 and 20: Instruction to disable an observer program if present (Fig 1, Fig 10, Col 5 lines 10-50, Col 19 line 15 – Col 20 line 65)

Entering a startup command to load a kill program before the observer program is started (Fig 10, Col 19 line 15 – Col 20 line 65) As shown within the figure the system clears the memory then loads a secondary extermination routine, inclusive of the secondary OS and associated extermination routine, so that the observer program is not reloaded and instead the kill program is loaded and executed.

Rebooting the computer (Fig 1, Fig 10) As it is shown after the detection and initial clearing of memory the system must be rebooted with a separate non-infected operating system to further allow for the deletion of any other virus elements..

Starting the kill program by execution of the startup command (Fig 10, Col 19 line 15 – Col 20 line 65) As explained above the kill program is loaded at startup so the virus may not load.

Deleting the observer program startup command and files (Fig 10, Col 19 line 15 – Col 20 line 65) The process of clearing the memory as stated within the cited lines and exterminating the malware is the process of deleting the startup command.

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Applicant is reminded that in amending in response to a rejection

of claims, the patentable novelty must be clearly shown in view of the state of art disclosed by the references cited and the objections made. Applicant must show how the amendments avoid such references and objections. See 37 CFR 1.111(c).

35. Inquiries concerning this communication or earlier communications from the examiner should be directed to Thomas M. Szymanski who can be reached at (571) 272-8574. The examiner's normal working schedule is between the hours 8:00am – 4:30pm (EST), Monday – Friday.

36. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

37. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JL

GREGORY MORSE
SUPERVISORY PATENT [illegible]
TECHNOLOGY [illegible]